UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/091,740	03/06/2002	Travis J. Parry	10013768-1	8466

7590 09/12/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
HOMAYOUNMEHR, FARID	
ART UNIT	**PAPER NUMBER**
2132	

MAIL DATE	DELIVERY MODE
09/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/091,740
Filing Date: March 06, 2002
Appellant(s): PARRY, TRAVIS J.

Charles Griggers
Registration No. 47,283
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 5/22/2007 appealing from the Office action mailed 1/18/2007.

(1) Real Party in Interest

The statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Following documents were relied upon in rejection of claims:

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

Claims 1, 2, 4-14, 17-30, 33-35, 37, 39-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Schwartz (US Patent Application Publication US 2002/0199114 A1).

10.1 As per claim 1, Schwartz is directed to a method of transmitting data across a firewall (paragraph [0013] line 1), the method comprising:
receiving a request to transmit data to a destination (paragraph [0028], where the client's attempt to open a connection discloses a request to transmit data); searching for a firewall associated with the destination (paragraph [0028] lines 8 to 11) at a remote network (for example, Fig. 3 item 314-5 is in network 311, which is associated with firewall 310, which is remote to client 308-1. See also paragraph 25), the firewall being configured to prohibit communication to the destination at a remote network via a primary communication protocol (Fig 4 and paragraph [0029] as disclosed by TCP port x, where the connection is not established), and allow communication to the destination via a secondary communication protocol (paragraph [0003], as it is describing the general functionality of a firewall); if the firewall is detected, automatically configuring the data for communication with the secondary communication protocol (paragraph [0029] line 1 to 5); and transmitting the data to the destination by utilizing the secondary communication protocol (paragraph [0029]), wherein the request to transmit data to the

destination comprises a primary address to the destination related to the primary communication protocol, and a secondary address to the destination related to the secondary communication protocol (paragraph [0028] and [0029], where, after the failure to connect via TCP (example of a primary protocol), the device tries to open a HTTP connection (example of the secondary protocol), and Schwartz claims 2 to 4 wherein the primary and secondary protocols use predefined addresses to initiate the connection and paragraphs [0040] and [0041], where the addresses are provided by the address database to the Communication Subsystem as communication parameters).

10.2. As per claim 2, Schwartz continues to teach the method of claim 1, further comprising: transmitting the data to the destination by utilizing the primary communication protocol if the firewall is not detected (paragraph [0029] line 1 to 5).

10.3. Claim 3 has been cancelled by the applicant.

10.4. As per claim 4, Schwartz discloses the method of claim 1, wherein the destination is a printer and a print job comprises the data that is requested to be transmitted. Printer is a computer peripheral that puts text or a computer-generated image on paper or on another medium, such as transparency film. Local printers communicate with the network via a PC, and network printers are directly connected to the network. Schwartz clearly discloses display and I/O devices (Fig. 2, item 220 and paragraph [0016]) as the parts comprising the clients' computer. In addition, Schwartz discloses traditionally

connected devices, which are devices configurable to communicate through the firewall, and non-traditional devices, which are devices that must be connected to another device (e.g. a PC) in order to communicate (paragraph [0024). Traditionally connected devices and non-traditional devices receive jobs in form of data directly or indirectly form the network, correspondingly. As indicated in Fig. 3, both traditionally connected and non-traditional devices are behind the firewall, and are disclosed as destinations for data to be transmitted across the firewall. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.5. As per claim 5, Schwartz discloses the method of claim 1, wherein searching for the firewall comprises pinging the primary address of the desired location. Pinging is sending out a small amount of information, or a packet, to a destination connected to the network, and examining the response to determine if the destination is responsive to network requests. Schwartz discloses initiation of a first connection and evaluating the connection for the response from the remote system (claim 1). More specifically, Pinging is sending out ICMP Echo Request Packets. Schwartz discloses ICMP as one of the protocols to initiate the first connection (claim 2). Therefore, the Examiner asserts that it discloses the feature.

10.6. As per claim 6, Schwartz discloses the method of claim 2, wherein searching for the firewall comprises:

scanning the desired location to find an open port, the open port being related

to the primary communication protocol; and detecting the firewall, if present, upon not finding the open port. Scanning is examining sequentially, part by part. As disclosed in Fig. 4, and described in paragraph [0029] the device that is transmitting the data examines the firewall by initiating connections using TCP, HTTP, and other options sequentially until a connection is established (Open port found). Therefore, it discloses the feature.

10.7. As per claim 7, Schwartz discloses the method of claim 2, wherein searching for the firewall comprises:

attempting to transmit the data via the primary communication protocol, such that a failure to successfully transmit the data via the primary communication protocol would signify the firewall is present. As described in Schwartz paragraph [0027], attempting to initiate a connection, involves transmitting data. Schwartz maintains that depending on the type of the communication protocol, different set of steps and data exchanges may be involved to determine whether a connection is established. Furthermore, when data transmission is unsuccessful, Schwartz tries another protocol (Fig. 4), which indicates that a firewall blocking the primary transmission is detected. Therefore it discloses the feature.

10.8. As per claim 8, Schwartz discloses the method of claim 2, wherein the primary communication protocol is any one or combination of the following:

the Hyper-Text Transfer Protocol (HTTP), the Transfer Control Protocol (TCP), the Internet Protocol (IP), the File Transfer Protocol (FTP), and the User Datagram Protocol (UDP). Schwartz clearly discloses primary communication protocols HTTP, TCP and UDP in claim 2, and IP in claim 10.

Schwartz recognizes and mentions FTP packets as another example of protocol data units examined and evaluated by firewalls (paragraph [0005]). Schwartz also refers to RFCs as other potential standards and protocols to be used as primary communication protocol (paragraph [0045]), one of which is RFC 959, The File Transfer Protocol. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.9. As per claim 9, Schwartz discloses the method of claim 1, wherein the secondary communication protocol is an
electronic mail (email) protocol (as disclosed in paragraph [0045], referring to RFCs for a list of potential protocols for communication, one of which is RFC 821, Simple Mail Transfer Protocol), and the secondary address is an email address (when SMTP is used as secondary communication protocol, an email address must be selected as the destination address); and further wherein automatically configuring the data for communication comprises: generating an email; addressing the email to the secondary address; and populating the email with pertinent information that correlates to the data. Data must be configured appropriately before transferred using any communication protocol. When email is used as the communication protocol, it is well

known that an email must be generated, addressed to the email address of the destination, and the data must be configured in the format that is suitable for email.

10.10. As per claim 10, Schwartz discloses the method of claim 9, wherein automatically configuring the data for communication further comprises: placing the data in the email (see section 3.9 above).

10.11. As per claim 11, Schwartz discloses the method of claim 9, wherein automatically configuring the data for communication further comprises: attaching the data to the email, the data being stored in a file (see section 3.9 above. Attachment is a well known way to configure data for transfer using email).

10.12. As per claim 12, Schwartz is directed to the method of claim 9, wherein the information that is populated in the email comprises a reference to a remote location where the data is stored and is accessible from the destination (in this case the data transmitted across the firewall is simply the data identifying the location of another data. Allowing access to data that is already accessible to the destination by identifying the location of the data is well-known in the art).

10.13. As per claim 13, Schwartz discloses the method of claim 1, wherein the secondary communication protocol is the File Transfer Protocol (FTP) and the secondary address is an FTP address. Schwartz recognizes and mentions FTP packets

as another example of protocol data units examined and evaluated by firewalls (paragraph [0005]). Schwartz also refers to RFCs as other potential standards and protocols to be used as primary communication protocol (paragraph [0045]), one of which is RFC 959, The File Transfer Protocol. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.14. As per claim 14, Schwartz is directed a system for rerouting the transmission of data to avoid a firewall (paragraph [0013] line 1), the system comprising: a transmission device configured to search for a firewall protecting a destination (paragraph [0028], where the client's attempt to open a connection discloses a request to transmit data) at a remote network (for example, Fig. 3 item 314-5 is in network 311, which is associated with firewall 310, which is remote to client 308-1. See also paragraph 25), the firewall at the remote network being configured to prohibit communication to the destination via a primary communication protocol searching for a firewall associated with the destination (paragraph [0028] lines 8 to 11), the firewall being configured to prohibit communication to the destination via a primary communication protocol (Fig 4 and paragraph [0029] as disclosed by TCP port x, where the connection is not established), and allow communication to the destination via a secondary communication protocol (paragraph [0003], as it is describing the general functionality of a firewall), the transmission device is further configured to, upon detection of the firewall, automatically configure the data for communication over the secondary communication protocol (paragraph [0029] line 1 to 5) and transmit the data by utilizing the secondary communication protocol

(paragraph [0029]), wherein the transmission device is further configured to receive a request to transmit data to the destination and the request comprises at least the following: a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol, and the secondary address being related to the secondary communication protocol (paragraph [0028] and [0029], where, after the failure to connect via TCP (example of a primary protocol), the device tries to open a HTTP connection (example of the secondary protocol), and Schwartz claims 2 to 4 wherein the primary and secondary protocols use predefined addresses to initiate the connection and paragraphs [0040] and [0041], where the addresses are provided by the address database to the Communication Subsystem as communication parameters), and wherein the transmission device is further configured to, upon not detecting the firewall, transmit the data to the destination by utilizing the primary transmission protocol (claim 1 indicates evaluation of the first connection, and trying the second if the first one was unsuccessful. Thus, if the evaluation shows that the transmission was successful, no firewall is detected and the transmission was done using the primary protocol).

10.15. Claim 15 is cancelled by the applicant.

10.16. Claim 16 is cancelled by the applicant.

10.17. As per claim 17, Schwartz is directed to the system of claim 14, wherein the transmission device is further configured to search for a firewall by scanning the destination to find an open port, the open port being related to the primary communication protocol, upon not finding the open port, the firewall is detected. Scanning is examining sequentially, part by part. As disclosed in Fig. 4, and described in paragraph [0029] the device examines the firewall by initiating connections using TCP, HTTP, and other options sequentially until a connection is established (Open port found). Therefore, it discloses the feature.

10.18. As per claim 18, Schwartz is directed to the system of claim 14, wherein the transmission device is further configured to search for a firewall by pinging the primary address of the destination. Pinging is sending out a small amount of information, or a packet, to a destination connected to the network, and examining the response to determine if the destination is responsive to network requests. Schwartz discloses initiation of a first connection and evaluating the connection for the response from the remote system (claim 1). More specifically, Pinging is sending out ICMP Echo Request Packets. Schwartz discloses ICMP as one of the protocols to initiate the first connection (claim 2). Therefore, the Examiner asserts that it discloses the feature.

10.19. As per claim 19, Schwartz is directed to the system of claim 14, wherein the transmission device is further configured to search for a firewall by attempting to transmit the data via the primary communication protocol, such that a failure to

successfully transmit the data via the primary communication protocol would signify the firewall is present. As described in paragraph [0027], attempting to initiate a connection, involves transmitting data. Schwartz maintains that depending on the type of the communication protocol, different set of steps and data exchanges may be involved to determine whether a connection is established. Furthermore, when data transmission is unsuccessful, Schwartz tries another protocol (Fig. 4), which indicates that a firewall blocking the primary transmission is detected. Therefore it discloses the feature.

10.20. As per claim 20 Schwartz discloses the system of claim 14, wherein the secondary communication protocol is an electronic mail (email) protocol (as disclosed in paragraph [0045], referring to RFCs for a list of potential protocols for communication, one of which is RFC 821, Simple Mail Transfer Protocol).

10.21. As per claim 21, Schwartz discloses the system of claim 20, wherein the secondary address is an email address (when SMTP is used as secondary communication protocol, an email address must be used as the destination address) and wherein the transmission device is further configured to automatically configure communication by: generating an email; addressing the email to the secondary address; and populating the email with pertinent information that correlates to the data. When email is used as the communication protocol, an email must be generated, addressed to the email address of the destination, and the data must be configured in the format that is suitable for email.

10.22. As per claim 22, Schwartz discloses the system of claim 21, wherein the transmission device is further configured to automatically configure the data for communication by placing the data in the email (see section 3.21 above).

10.23. As per claim 23, Schwartz discloses the system of claim 21, wherein the transmission device is further configured to automatically configure the data for communication by attaching the data to the email, the data being stored in a file (see section 3.21 above. Attachment is a well know method to configure data for transfer using email).

10.24. As per claim 24, Schwartz is directed to the system of claim 21, wherein the information that is populated in the email comprises a reference to a remote location where the data is stored and is accessible from the destination (in this case the data transmitted across the firewall is simply the data identifying the location of another data. Allowing access to data that is already accessible to the destination by identifying the location of the data is well-known in the art).

10.25. As per claim 25, Schwartz is directed to the system of claim 14, wherein the secondary communication protocol is the File Transfer Protocol (FTP) and wherein the secondary address is an FTP address. Schwartz recognizes and mentions FTP packets as another example of protocol data units examined and evaluated by firewalls

(paragraph [0005]). Schwartz also refers to RFCs as other potential standards and protocols to be used as primary communication protocol (paragraph [0045]), one of which is RFC 959, The File Transfer Protocol. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.26. As per claim 26, Schwartz discloses the system of claim 14, wherein the primary communication protocol is any one or combination of the following: the Hyper-Text Transfer Protocol (HTTP), the Transfer Control Protocol (TCP), the Internet Protocol (IP), the File Transfer Protocol (FTP), and the User Datagram Protocol (UDP). Schwartz clearly discloses primary communication protocols HTTP, TCP and UDP in claim 2, and IP in claim 10.

Schwartz recognizes and mentions FTP packets as another example of protocol data units examined and evaluated by firewalls (paragraph [0005]). Schwartz also refers to RFCs as other potential standards and protocols to be used as primary communication protocol (paragraph [0045]), one of which is RFC 959, The File Transfer Protocol. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.27. As per claim 27, Schwartz discloses the system of claim 14, further comprising: a recipient device configured to be the destination, the recipient device further configured to communicate with the primary and secondary communication protocol (Fig. 4 and paragraph [0027]).

10.28. As per claim 28, Schwartz is directed to the system of claim 27, wherein the recipient device is a printer and a print job comprises the data. Printer is a computer peripheral that puts text or a computer-generated image on paper or on another medium, such as transparency film. Local printers communicate with the network via a PC, and network printers are directly connected to the network. Schwartz clearly discloses display and I/O devices (Fig. 2, item 220 and paragraph [0016]) as the parts comprising the clients' computer. In addition, Schwartz discloses traditionally connected devices, which are devices configurable to communicate through the firewall, and non-traditional devices, which are devices that must be connected to another device (e.g. a PC) in order to communicate (paragraph [0024). Traditionally connected devices and non-traditional devices receive jobs in form of data directly or indirectly form the network, correspondingly. As indicated in Fig. 3, both traditionally connected and non-traditional devices are behind the firewall, and are disclosed as destinations for data to be transmitted across the firewall. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.29. As per claim 29, Schwartz is directed to a transmission device configured to transmit data to a destination, the transmission device comprising: means for transmitting the data to a destination at a remote network (for example, Fig. 3 item 314-5 is in network 311, which is associated with firewall 310, which is remote to client 308-1. See also paragraph 25) by utilizing a secondary communication protocol (paragraph

[0029]), means for searching for a firewall at a remote network (paragraph [0028] lines 8 to 11), the firewall being configured to prohibit communication to the destination by a primary communication protocol (Fig 4 and paragraph [0029] as disclosed by TCP port x, where the connection is not established), and allow communication to the destination via the secondary communication protocol (paragraph [0003], as it is describing the general functionality if a firewall); and means for automatically configuring the data for communication for the secondary communication protocol upon detecting the firewall (paragraph [0029] line 1 to 5) and

means for receiving a request to transmit the data to the destination, wherein the request comprises at least the following:

a primary address to the destination related to the primary communication protocol, and a secondary address to the destination related to the secondary communication protocol (paragraph [0028] and [0029], where, after the failure to connect via TCP (example of a primary protocol), the device tries to open a HTTP connection (example of the secondary protocol), and Schwartz claims 2 to 4 wherein the primary and secondary protocols use predefined addresses to initiate the connection and paragraphs [0040] and [0041], where the addresses are provided by the address database to the Communication Subsystem as communication parameters).

10.30. As per claim 30, Schwartz is directed to the device of claim 29, further comprising means for transmitting the data by utilizing the primary communication

protocol, wherein upon not detecting the firewall, the data is transmitted by utilizing the primary communication protocol (paragraph [0029] line 1 to 5).

10.31. Claim 31 is cancelled by the applicant.

10.32. Claim 32 is cancelled by the applicant.

10.33. As per claim 33, Schwartz is directed to the device of claim 30, wherein the secondary communication protocol is an electronic mail (email) protocol (as disclosed in paragraph [0045], referring to RFCs for a list of potential protocols for communication, one of which is RFC 821, Simple Mail Transfer Protocol).

10.34. As per claim 34, Schwartz is directed to the device of claim 30, wherein the secondary address is an email address (when email is the means to transfer information, and SMTP is used as secondary communication protocol, an email address must be used as destination address), and wherein the means for automatically configuring the data for communication for the secondary communication protocol comprises: means for generating an email, means for addressing the email to the secondary address; means for populating the email with pertinent information that correlates to the data; and means for populating the email with the data . Data must be configured appropriately before transferred using any communication protocol. When email is used as the means to transfer data an email must be generated, addressed to

the email address of the destination, and the data must be configured in the format that is suitable for email.

10.35. As per claim 35, Schwartz is directed to a data transmission program stored on a computer-readable medium (paragraph [0014]), the transmission program comprising: logic configured to facilitate the transmission of data to a remote network (item 314-5 in the network 311, which is remote from client 308-1) by utilizing a secondary communication protocol (paragraph [0029]); logic configured to search for a firewall (paragraph [0028] lines 8 to 11) at a remote network (for example, Fig. 3 item 314-5 is in network 311, which is associated with firewall 310, which is remote to client 308-1. See also paragraph 25), wherein the firewall is configured to prohibit communication to a recipient device at a remote network via a primary communication protocol and allow a communication via the secondary protocol (paragraph [0028])
and logic configured to automatically configure communication for the secondary communication protocol upon detecting the firewall (paragraph [0029]) and
logic configured to receive a request to transmit the data to the recipient device, the request comprising at least of the following:
a primary address to the destination related to the primary communication protocol, and a secondary address to the destination related to the secondary communication protocol (paragraph [0028] and [0029], where, after the failure to connect via TCP (example of a primary protocol), the device tries to open a HTTP connection (example of the secondary protocol), and Schwartz claims 2 to 4 wherein the primary and

secondary protocols use predefined addresses to initiate the connection and paragraphs [0040] and [0041], where the addresses are provided by the address database to the Communication Subsystem as communication parameters).

10.36. Claim 36 is cancelled by the applicant.

10.35. As per claim 37, Schwartz is directed to the program of claim 35, further comprising logic configured to facilitate the transmission of the data by utilizing the primary communication protocol, wherein upon not detecting the firewall, the data is transmitted by utilizing the primary communication protocol (paragraph [0029] line 1 to 5).

10.38. Claim 38 is cancelled by the applicant.

10.39. As per claim 39, Schwartz is directed to the program of claim 35, wherein the secondary address is an electronic mail (email) address (which must be the case when communication protocol is email) and the secondary communication protocol is an email protocol (as disclosed in paragraph [0045], referring to RFCs for a list of potential protocols for communication, one of which is RFC 821, Simple Mail Transfer Protocol); and wherein the logic configured to automatically configure the data for communication for the secondary communication protocol comprises: logic configured to generate an email; logic configured to address the email to the secondary address; logic configured

to populate the email with pertinent information that correlates to the data; and logic configured to populate the email with the data. Data must be configured appropriately before transferred using any communication protocol. When email is used as the communication protocol, it would be obvious to a person with ordinary skills in the art that an email must be generated, addressed to the email address of the destination, and the data must be configured in the format that is suitable for email.

10.40. As per claim 40, Schwartz is directed to the program of claim 35, wherein the secondary communication protocol is the File Transfer Protocol (FTP) and the secondary address is an FTP address. Schwartz recognizes and mentions FTP packets as another example of protocol data units examined and evaluated by firewalls (paragraph [0005]). Schwartz also refers to RFCs as other potential standards and protocols to be used as primary communication protocol (paragraph [0045]), one of which is RFC 959, The File Transfer Protocol. Therefore, the Examiner asserts that Schwartz discloses the feature.

10.41. As per claim 41, Schwartz is directed to the program of claim 35, wherein the primary communication protocol is any one or combination of the following: the Hyper-Text Transfer Protocol (HTTP), the Transfer Control Protocol (TCP), the Internet Protocol (IP), the File Transfer Protocol (FTP), and the User Datagram Protocol (UDP). Schwartz clearly discloses primary communication protocols HTTP, TCP and UDP in claim 2, and IP in claim 10.

Schwartz recognizes and mentions FTP packets as another example of protocol data units examined and evaluated by firewalls (paragraph [0005]). Schwartz also refers to RFCs as other potential standards and protocols to be used as primary communication protocol (paragraph [0045]), one of which is RFC 959, The File Transfer Protocol. Therefore, the Examiner asserts that Schwartz discloses the feature.

(10) Response to Argument

In response to rejections under 35 U.S.C. 102(e) as being anticipated by Schwartz (US Patent Application Publication US 2002/0199114 A, filed Jan. 26, 2002), the appellant has argued the following:

With respect to claim 1, appellant argues that Schwartz does not teach the limitation of claim 1. Appellant argues: "Rather, *Schwartz* discloses at most a system for configuring a device to communicate through a firewall on a local network, where the device is also located on the local network. *See* paras. 0024-0025. *See* Figure 3 *(e.g.,* devices 312, 314, and firewall 310). *Schwartz* fails to teach or suggest searching for a firewall associated with a destination at a remote network." Specifically, applicant argues that the scope of Schwartz disclosure is limited to local networks and firewalls associated with local device, and does not include firewalls associated with remote devices. However, Schwartz disclosure is related to

traversing a firewall (see parag. 7, 13, or 42, or Schwartz claim 1) in a local or remote network (see parag. 15 or 6). In fact Schwartz paragraph 15 reads:

"*The method and apparatus described herein may be applied to essentially any type of communicating means or device whether* ***local or remote****, such as a LAN, a WAN, a computer, an appliance, a home security system, a disk drive, a home computing environment, an entertainment system, media storage, etc.*"

Therefore, Schwartz firewall traversal techniques are clearly applicable to firewalls associated with local or **remote** devices. Note also that appellant's invention **searches** for a firewall associated with a destination by trying the first address to see if the connection failed, and if it did, it tries another address (see for example appellant's claim 7). Schwartz invention includes the exact equivalent of such search as shown in the protocol depicted in Fig. 4 and parag. 28.

Appellant's cited paragraphs 0024 and 0025 show that Schwartz teachings are applicable to a local network, and they also teach that the teachings are applicable to remote network. Paragraph 25 teaches several example scenarios that a local device traverses a firewall to connect to a remote device. It also teaches that the local device may receive an advertisement telling the consumer how and when to purchase a product. Therefore, the consumer **receives** an advertisement from remote server. In this case, the receiving device is located in a remote network with respect to the server. The server sends an advertisement to a device located in a remote network, and has to

traverse the firewall associated with the device. Note that as mentioned in paragraph 6, an external device attempting to reach an internal resource behind the firewall is presented with the need to get through the firewall. Therefore, Schwartz teaches that the server sends advertisement to the device behind the firewall and that sending the advertisement requires traversing the firewall. The bi-directional nature of exampled communications is explicitly indicated in paragraph 0025. Therefore, Schwartz teaches a system for traversing a firewall associated with a device in a remote network.

As another example, note that the request to transmit data across a firewall is received at the module responsible for establishing communication at the device which is transmitting data across the firewall. Therefore an internal module within the transmitting device receives the request. An example of this is shown in Fig. 6, and associated paragraphs 39 to 41. The main system 602 uses the communication subsystem 606 to establish a communication. Therefore the request goes to communication subsystem 606. Therefore, when any device (local or remote) transmits, the request is received by a module within that same device. Note that there is no requirement in the claim that the request for traversal must be performed by a separate server that is specialized for firewall traversal. A transmitting device performing the firewall traversal protocol by itself meets the claim requirement.

Applicant further argues: "*Schwartz* also states that "if an address and/or port does not yield a successful connection, then the next time the device will select the most likely address and port

506, it may not include the unsuccessful port." *See* para. 0032. "It is to be understood that select most likely address and port 506 is based upon a database of addresses and ports and that this database changes." *See* para. 0032. Therefore, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address of the destination that is used if a firewall is not detected and a secondary address of the destination that is used if a firewall is detected, as described in the claim. Rather, *Schwartz* uses whatever port the non-traditional device discerns is most likely to establish a connection with the local firewall. As such, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address and a secondary address of a firewall associated with a destination." However, The claim requirement does not mention the address of a **firewall** associated with a destination. The claim requires the request to include the primary and secondary address of **a destination device** associated with the firewall. The address of the firewall is not in the claim requirement. It is the address of the destination device. Schwartz does teach a request to transmit data to the destination device, including the primary and secondary address of the destination device. As shown in the above cited portion of appellant's argument, appellant admits that Schwartz first tries a protocol, and if an address and/or port does not yield a successful connection, then the device tries another address. Therefore, Schwartz tries a first address and then another address associated with the destination device. Also, see Schwartz paragraph 0029 clearly showing how different protocols are tried to traverse the firewall. It also shows that the address of the destination device associated with each said protocol (TCP, HTTP, and HTTP via a proxy) is tried in the effort to traverse the firewall.

Appellant further argues: "As previously indicated, *Schwartz* teaches that a local device is configured to operate with a local firewall by attempting different addresses for the local firewall. Nowhere does it teach or suggest attempting to communicate with a firewall associated with a destination at a remote network in a manner described by the claim." However, Appellant has not shown any reason that the system is only applicable to, or works only with a local device. As described before, Schwartz teaches a firewall traversal method for traversing firewalls associated with devices located in both local and remote network.

Appellant further argues: "However, nowhere in *Schwartz* does it state that the clients 308-1...308-N shown in Fig. 3 perform the method for firewall traversal disclosed in the reference. Rather, the non-traditional devices 314-1...314-Q are disclosed to employ the method for firewall traversal described in the reference which states "This information must be transferred from the non-traditional device across the LAN 311 through the firewall 310 to a destination." Para. 0025." However, the cited portion of paragraph 0025 shows a local device traversing a firewall to reach remote device. As discussed previously, Schwartz also teaches the bi-direction communication, which requires the clients and servers in Fig. 3, must traverse the firewall to reach the local devices. An example of communication form the server to local devices is, as stated previously, when the server sends the local device advertisements, or music to be played by the local entertainment system.

Appellant further argues: "Moreover, the Office Action of July 24, 2006 states that "It is true that Scharwtz won't try the primary address again if it fails, but it clearly tries it the first time, which was before the connection failed. Therefore, the address of the primary and secondary protocols must be received by the device that initiates the connection." Page 4. Applicant respectfully disagrees, since *Schwartz* teaches that an address may be obtained by sniffing network traffic and therefore does not have to be "received by the device that initiates the connection." Further, *Schwartz* does not teach or suggest that a request to transmit data comprises both the primary address and secondary address of the destination, as described in claim 1." However, it is not clear how the fact that the address may be found via sniffing the network proves that the address does not have to be received by the device that initiates the connection. The destination addresses are provided to the device that initiates the connection as part of the communication protocol requirement (TCP or HTTP), and as described in paragraph 0029.

Appellant further continues: "Further, *Schwartz* does not teach or suggest that a request to transmit data comprises both the primary address and secondary address of the destination, as described in claim 1." However, Schwartz teaches a firewall traversal method which tries to establish a connection by trying multiple protocols and using the destination addresses associated with each protocol. Therefore, *Schwartz* teaches a request to transmit data comprising both the primary address and secondary address of the destination, as described in claim 1.

Appellant continues to argue that Schwartz teachings are just limited to a local device traversing a firewall. Applicant argues: "However, *Schwartz* does not describe that a client 308-N attempts to build a database of addresses and ports for a remote firewall 311 by sniffing network traffic. Rather, *Schwartz* teaches that the non-traditional devices 314-N attempt to build a database of addresses and ports for the local firewall 311 by sniffing local network traffic. *See* paras. 0033-0034. This is because *Schwartz* is focused on a local client device attempting to find a port of a local firewall that allows the client device to communicate with remote devices. *See* para. 0034." However, paragraphs 33 and 34 do not limit their teachings to local device 314-N. The teachings in paragraphs 33 and 34 are related to a way of prioritizing the addresses such that the address with the highest chance of success is tried first. As discussed before, Schwartz teachings include a firewall traversal method to traverse a firewall associated with both a local and remote devices.

Applicant further cites a portion of Examiner's Final Rejection and concludes that Examiner has allegedly failed to show that Schwartz teaches a request to transmit data to destination comprises both a primary address of the destination and a secondary address of the destination. However, Examiner's response in the Final Action is not limited to the cited portion by the appellant. Examiner's Final Action in pages 4 and 5 cites Schwartz paragraph 30, showing teaching of a computer based system, which opens a connection between a source and a destination. The opening of a connection as taught by Schwartz involves trying a first destination address, and the second destination address, as it includes trying the destination address of at least three

different protocols (see Fig. 4). The computer based system configures an Ethernet adapter to establish the communication. Therefore, the Ethernet card receives a request to make a connection including the addresses to try and make the connection. Examiner's Final Action includes another example embodiment of Schwartz, teaching said requirements. Cited paragraphs 39 and 40 show an example embodiment depicted in Fig. 6. In Fig. 6 the operation of Schwartz system is depicted in separate modules, including a main system 602, a database system 610, and a communication subsystem 606. Each module has a separate and well defined functionality. As described in paragraphs 39 and 40, the main system tries to open a connection using the communication subsystem 606. Therefore, the communication subsystem does not decide to make a connection on its own. It is the main system 602 that attempts the connection, using the communication subsystem 606. Therefore, the communication subsystem 606 receives a request to make the connection. This request contains the addresses to be tried for establishing the communication, as the communication subsystem 606 does not have the address. Note that as explained in paragraphs 40 and 41, these addresses are stored in the database module 610, and are delivered to communication subsystem 606 when it is configured to open a connection by the main system 602.

Appellant's arguments with respect to claims 2, 4-13 is based on allowability of claim 1. Appellant does point out that said claims include additional requirements, but presents

no argument on how they are distinguished from the prior art, or traverse the associated rejections. Therefore, claims 2, 4-13 stand or fall together with claim 1.

Appellant's arguments relative to claims 14, 17-30, 33-35, 37, 39-41 are substantially identical to their arguments discussed above.

Based on the discussion above, appellant's arguments are not persuasive, and the rejections should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

/Farid Homayounmehr/

August 28, 2007

Conferees:

Gilberto Barron

Matthew Smithers

/Matthew Smithers/
Primary Examiner
Art Unit 2137